UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/865,667	05/29/2001	Michael G. Lee	57983.000041	4126

7590 02/13/2007

Thomas E. Anderson
Hunton & Williams
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	02/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/865,667
Filing Date: May 29, 2001
Appellant(s): LEE ET AL.

Thomas Anderson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 21 September 2006 appealing from the Office action mailed 28 February 2006.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,546,486	**PERLMAN ET AL**	**8-2003**
6,438,612	**YLONEN ET AL**	**8-2002**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-2, 4-8, and 10-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Perlman et al US Patent No. 6,546,486. Perlman discloses a content screening system with end to end encryption.

With regards to claims 1 and 7, Perlman discloses the detecting of an exchange of a first encryption key between a host device and a remote device wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (Perlman, column 4 lines 63-66, message key), exchanging a second key with the host device when the exchange of the first encryption key is detected wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged an entity and the host device according to a second security policy (Perlman, column 5 line 66 – column 6 line 4), requesting at the firewall, based at least in part upon the second security policy, the first encryption key wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security

policy (Perlman, column 6 lines 48-63), and passing encrypted data when it is determined that the first encryption key is received (Perlman, column 5 lines 20-22).

With regards to claims 2 and 8, Perlman teaches not allowing encrypted data to pass when it is determined that the first encryption key is not received (Perlman, column 9 lines 15-22).

With regards to claims 4 and 10, Perlman teaches everything described above and further teaches the decrypting of encrypted data using the first encryption key according to a predetermined monitoring policy (Perlman, column 6 lines 19-34).

With regards to claims 5 and 11, Perlman teaches everything described above and further teaches the applying of a predetermined filtering policy to the decrypted data (Perlman, column 6 lines 19-34).

With regards to claims 6 and 12, Perlman teaches the re-encrypting of the decrypted data (Perlman, column 9 lines 15-22).

Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al US Patent No. 6,546,486 in view of Ylonen et al US Patent No. 6,438,612.

With regards to claims 3 and 9, Perlman fails to teach the use of Internet Key Exchange protocol data traffic to determine when the first key is exchanged. Ylonen teaches the use of Internet Key Exchange protocol data traffic to determine when a key is exchanged (Ylonen, column 5 line 56 – column 6 line 5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ylonen's method of using the IKE protocol with Perlman's content screening system

because it offers the advantage of using a key management scheme that provides authentication between source and destination while adhering to an industry standard method of key exchange (Ylonen, column 4 lines 39-59).

(10) Response to Argument

Applicant has provided arguments directed towards the 35 USC § 102 rejection of claims 1, 2, 4-8, and 10-12 and has alleged that the Examiner has failed to establish a prima facie case of obviousness against claims 3 and 9. Examiner respectfully disagrees with Applicant's arguments and maintains that Perlman et al US Patent No. 6,546,486 (hereafter "Perlman") anticipates claims 1, 2, 4-8, and 10-12 and that Perlman in combination of Ylonen et al US Patent No. 6,438,612 (hereafter "Ylonen"" renders claims 3 and 9 unpatentable in view of 35 USC § 103.

PERLMAN ANTICIPATES CLAIMS 1, 2, 4-8, AND 10-12

Applicant has argued on pages 11-16 against the anticipation of claims 1, 2, 4-8, and 10-12 by asserting that Perlman fails to teach detecting an exchange of a first encryption key between a host device and a remote device, exchanging a second encryption key with the host device, and not allowing encrypted data to pass when it is determined that the first encryption key is not received. Examiner respectfully disagrees.

Perlman teaches detecting an exchange of a first encryption key between a host device and a remote device (Perlman, column 6 lines 4-13). Perlman teaches that a first encryption key (Perlman, column 6 line 7, message key Item 204) is first exchanged between a host and a remote device (Perlman, column 6 lines 4-13, source and destination) and as a result of the exchange a second exchange of the first encryption key between the firewall and either the host or remote device occurs (Perlman, column 6 lines 10-14). The second exchange of the message key is conditional upon the first exchange of the message key and thus the first exchange must have been detected. It should further be noted that the claims as currently presented do not define where the "detecting" step occurs. Given its broadest reasonable interpretation, the detection may reasonably be interpreted to occur in the claimed host, remote device, or firewall. Hence, the detection occurs in the host when the host sends the first encryption key to the remote device (Perlman, column 6 lines 4-10) and once detected, the host and the firewall then engage in a second key exchange (Perlman, column 6 lines 10-14).

Perlman also teaches exchanging a second encryption key with the host device (Perlman, column 6 lines 10-14, "secure manner", column 5 line line 65 – column 6 line 4). Perlman discloses the exchanging of a second key (Perlman, column 5 line line 65 – column 6 line 4, firewall public key) once the exchange of the first key is detected (Perlman, column 6 lines 10-14). Perlman discloses that once the exchange of the first message key occurs between the source and destination *then* the message key is exchanged between the source or destination and the firewall *in a secure manner.* Perlman describes *the secure manner* by disclosing that the firewall public key is used

by the host to encrypt the message key to be sent to the firewall (Perlman, column 5 line line 66 – column 6 line 4). Accordingly, a second key in the form of the firewall public key must be exchanged with the host device to allow the host device to then encrypt the first encryption key and send the encrypted first encryption key to the firewall. Thus, Perlman teaches exchanging a second encryption key with the host device (Perlman, column 6 lines 10-14, "secure manner", column 5 line line 65 – column 6 line 4, firewall public key).

Perlman teaches not allowing encrypted data to pass when it is determined that the first encryption key is not received (Perlman, column 9 lines 15-22, column 6 lines 34-36). Perlman discloses preventing encrypted data to pass by teaching that encrypted data will not be forwarded to the destination unless the encrypted message satisfies the screening criterion on the firewall (Perlman, column 6 lines 34-36). Hence, a failure in screening by the firewall causes the firewall to not pass encrypted data. Since the firewall cannot screen encrypted data if the first encryption key is not received, Perlman satisfies the limitation that if the first encryption key is not received encrypted data will not be passed by the firewall.

EXAMINER HAS ESTABLISHED A PRIMA FACIE CASE OF OBVIOUSNESS AGAINST CLAIMS 3 AND 9

Applicant has argued on pages 17-19 that the combination of Perlman and Ylonen fails to render claims 3 and 9 unpatentable. Applicant asserts that Perlman fails

to disclose the limitations noted above regarding the rejection under 35 USC § 102 and further asserts that Ylonen fails to teach "monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchange." Examiner respectfully disagrees.

As noted above, Perlman teaches the detecting of whether a first encryption key is exchanged (Perlman, column 6 lines 4-14). However, Perlman fails to teach the use of the IKE protocol. Ylonen remedies this deficiency by teaching the use of the IKE protocol to exchange keys (Ylonen, column 5 line 55 – column 6 line 5). Hence, Perlman teaches the detecting of the exchange of a key while Ylonen teaches the exchanging of keys using the IKE protocol. Together, Perlman and Ylonen teach monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchange (Perlman, column 6 lines 4-14, Ylonen, column 5 line 55 – column 6 line 5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified Perlman's key exchange system with Ylonen's Internet Key Exchange (IKE) protocol because it offers the advantage of using a key management scheme that provides authentication between source and destination while adhering to an industry standard method of key exchange (Ylonen, column 4 lines 39-59). Perlman and Ylonen teach every single limitation of claims 3 and 9 and motivation for the combination has been provided from within the references. Thus, Examiner has established a prima facie case of obviousness against claims 3 and 9 using Perlman and Ylonen.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

ALN

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Andrew Nalven ALN

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron GB

Matthew Smithers MS